

☒ Return Receipt Postcard

☐ Preliminary Amendment

☐ Please cancel filed claims _____.

☐ Incorporation by Reference (for Continuation/Division application) The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

☐ Since the present application is based on a prior US application, please amend the specification by adding the following sentence before the first sentence of the specification: "The present application is based on prior US application No. _____, filed on _____, which is hereby incorporated by reference, and priority thereto for common subject matter is hereby claimed."

☒ The filing fee is calculated as follows:

CLAIMS AS FILED, LESS ANY CANCELED BY AMENDMENT

	NUMBER OF CLAIMS	NUMBER EXTRA	RATE	FEE
TOTAL CLAIMS	38 - 20 =	18	X \$18	= \$324.00
INDEPENDENT CLAIMS	2 - 3 =	0	X \$78	= \$0.00
MULTIPLE DEPENDENT CLAIMS			\$260	= \$0.00
			BASIC FEE	=\$ 690.00
			TOTAL FILING FEE	=\$ 1014.00

☒ Please charge Deposit Account No. 13-4772 in the amount of \$ 1014.00 for the Total Filing Fee.

☒ The Commissioner is hereby authorized to charge any additional fees which may be required now or in the future under 37 CFR 1.16 or 37 CFR 1.17, including any present or future time extension fees which may be required, or credit any overpayment to Deposit Account No. 13-4772

☒ One additional copy of this sheet is enclosed

Please forward all correspondence to:

Customer Number **22917**

By: 

Kenneth A. Haas
Attorney for Applicant(s)
Registration No. 42,614
MOTOROLA, INC.
Phone: (847) 576-0379
Fax: (847) 576-3750

INVENTOR INFORMATION

Inventor One Given Name:: Robert
Family Name:: Banks
Postal Address Line One:: 4921 Lichfield Drive
City:: Barrington
State or Province:: Illinois
Country:: USA
Postal or Zip Code:: 60010-5615
City of Residence:: Barrington
State or Province of Residence:: Illinois
Country of Residence:: USA
Citizenship Country:: USA
Inventor Two Given Name:: Wesley S
Family Name:: Jones
Postal Address Line One:: 643 East Monterey Road
City:: Palatine
State or Province:: Illinois
Country:: USA
Postal or Zip Code:: 60067-3725
City of Residence:: Palatine
State or Province of Residence:: Illinois
Country of Residence:: USA
Citizenship Country:: USA
Inventor Three Given Name:: Richard
Family Name:: Malcolm
Postal Address Line One:: 625 Paxton Place
City:: Carol Stream
State or Province:: Illinois
Country:: USA
Postal or Zip Code:: 60188
City of Residence:: Carol Stream
State or Province of Residence:: Illinois
Country of Residence:: USA
Citizenship Country:: USA

CORRESPONDENCE INFORMATION

Correspondence Customer Number:: 22917
Fax One:: (847) 576-3750

APPLICATION INFORMATION

Title Line One:: Method and Apparatus for Interfacing a N
Title Line Two:: etwork to an External Element
Total Drawing Sheets:: 2
Formal Drawings?: Yes
Application Type:: Utility
Docket Number:: CE08314R

[illegible][illegible][illegible][illegible]

**METHOD AND APPARATUS FOR INTERFACING A NETWORK TO AN
EXTERNAL ELEMENT**

Field of the Invention

5 The invention relates generally to communication networks, and more particularly, the invention relates to a method and apparatus for interfacing a communication network to an external element.

10 Background of the Invention

 A communication network is typically designed to provide a vast array of functions and services to the users of the network. At the same time, new functions and features are conceived and developed that may enhance the communication network. Some of these new functions may lie outside the architecture of the existing communication network. Adaptation of these new functions to the communication network may require costly redesign and implementation of the communication network. Moreover, the communication network may be designed with a proprietary architecture and data structure that limits an ability to directly integrate these newly developed functions.

 Other desirable features and functions may be resident within other networks external to the communication network. Benefits may be derived from providing these features and functions within the communication network, or to at least permit users of the communication network to utilize these features and functions that reside on the external network.

30 Certain communication network architectures are designed with a view toward feature extraction. Feature extraction refers to the adaptability of the network to new services, features and functions that may be developed by

virtually anyone including service providers, system operators, third party vendors and end-users.

To permit adaptation of newly developed functionality to the communication network, and/or to permit utilization of external network functionality by users of the communication network, it is necessary to interface the new functions to the communication network in a stable and secure manner.

Thus, there is a need for a method and apparatus for interfacing a network to an external element in a stable and secure manner.

Brief Description of the Drawings

FIG. 1 is a block diagram illustration of a communication network coupled to an external element by an apparatus in accordance with a preferred embodiment of the present invention.

FIG. 2 is a functional block diagram illustrating the interface of an external element to a communication network in accordance with a preferred embodiment of the present invention.

FIG. 3 is a functional block diagram illustration of a services delivery element in accordance with a preferred embodiment of the invention.

FIG. 4 is a functional block diagram of a services delivery element in accordance with one of the preferred embodiments of the invention illustrating further functionality of the services delivery element.

FIG. 5 is a functional block diagram illustrating services invocation between a communication network and an external element in accordance with one of the preferred embodiments of the present invention.

FIG. 6 is a block diagram illustration of a communication network coupled to an external element by an apparatus in accordance with a preferred embodiment of the present invention.

5

Detailed Description of the Preferred Embodiments

A services delivery element forms an interface or operates as an interface device between an external element (such as an external end user's network feature server) and a communication network including both a core network and at least one access network. The services delivery element provides access to the core network, access networks and subscriber devices within or connected to the access networks to which the external element is interfaced. In accordance with a first aspect of the invention, the services delivery element acts as a security proxy and a secure link point between the external element and the core network. The services delivery element may also provide managed access by the external element to core network and access network resources. In addition to the above-described features, the services delivery element may also recognize or identify trusted external elements; identify preferential external elements; provide secure access to subscriber data retained within the core network; identify and deny access by untrusted external elements; translate between the external element and the core network; and provide limited access to particular subsets of core network data and/or functions by the external element.

With reference to FIG. 1, a core network 10 is interfaced to an access network 12. The core network 10 may be a packet based communication network adapted to provide voice and data communication services via the

access network 12, which may be a radio access network. A radio access network provides wireless voice and data communication services to a mobile unit, such as the mobile unit 14, and may do so in accordance with virtually any wireless communication protocol. The invention provides an interface for external elements to both the core network 10, the access network 12, and the mobile unit 14. To simplify the following discussion of the preferred embodiments of the invention, reference is made only to the core network 10.

Referring to FIG. 1 and FIG. 2, within the core network 10 is a variety of application program interfaces (API) 18, which interface services and functional components within the core network 10. As shown in FIG. 2, for example, is a call model API 19 and a resource API 20. Each of API 19 and API 20 are considered to be internal APIs, and as such have "trusted" status within the core network 10. That is, these APIs have access to the core network 10 without having to first authenticate and establish a secure interface with the core network. Also illustrated in FIG. 2 are external APIs 22, such as applications API 23 and services API 24. While only two external APIs 23 and 24 are shown, it should be understood that numerous external APIs might be provided.

External APIs 22 are considered "untrusted" APIs and do not have the same, direct access to the core network 10 as the trusted, internal APIs 18. The internal APIs 18 may be considered the "glue" of core network 10, which enable the features and services in the core network 10. As an example, the internal APIs support the configuration of the communication between the network entities (not shown) within the core network 10.

In contrast, the external APIs 22 are accessible to and configurable by third parties, e.g., services providers and, where appropriate, end users. The external APIs 22 are the feature extraction pieces that enable third party
5 developers to access and add features and services to the network. The external APIs 22 interface with the internal APIs 18 to configure, communicate with and control the network to provide extensibility to the core network 10. In accordance with a preferred embodiment of the invention,
10 the external APIs 22 and internal APIs 18 are linked together via a services delivery element 26. The services delivery element 26 segregates the sets of APIs, and has a primary purpose to provide security for the internal APIs from untrusted resources.

15 Because the external APIs 22 connect to the core network 10, it is possible that mechanisms may be added to the core network 10 via these external APIs 22, that can be damaging or even totally destructive. Any service, not resident within the core network 10, that requires the
20 execution of programmable code, that requires processing from a core network entity, or data access on behalf of a subscriber from the core, is considered external. These services, such as the Call Processing Language from the IPTEL working group of the Internet Engineering Task Force
25 (IETF) or some features of the Wireless Application Protocol(WAP), enable end users to load executable code into the network. These services cannot be trusted and should not be granted direct access to the core network 10.

30 As discussed above, the internal APIs 18 are the system interfaces which enable features and services in the core network 10. The internal APIs 18 address the configuration of and communication between the network

entities inside both the core and access networks 10 and 12. These interfaces will not be directly accessible external to the core network 10.

The services delivery element 26 protects the core network 10 from potentially destructive features and services, and further provides indirect access to the internal APIs 18. FIG. 3 illustrates a functional architecture for the services delivery element 26 in accordance with a preferred embodiment of the invention.

The services delivery element 26 may include both a security services element 302 and a translation/API modules element 304. One of ordinary skill in the art will appreciate that FIG. 3 represents the functional elements of the services delivery element 26, and that in an actual physical embodiment of the services delivery element 26, these functional elements may reside in one or more components of the core network 10.

The security services element 302 provides authentication and validation services to potential service and feature providers of the network. In accordance with the preferred embodiments of the invention, access to the core network 10 by external elements, i.e., external APIs 22, are via a secure connection across a virtual private network (VPN) connection. The security services element 302 adds a wrapper on top of the internal API that will enable the external feature or service. This arrangement allows the external feature or service to have scalable access to the internal API 18, but through a secure technique. Access to the internal API 18 by the external elements ranges from no access to partial access to full access based on a variety of security variables. These variables include user based privileges (e.g., service

-7-

options based on subscription information) and network variables (e.g., based on network usage and load). More generally speaking, the services delivery element 26 enables a layering of restrictions providing greater or
5 lesser authorization to the external element based upon virtually any set of criteria, including without limitations those set forth above.

The connection security between the external API 22 and the internal API 18 may be provided using the IP
10 security protocol (IPSec) from the Internet Engineering Task Force (IETF). Utilizing both the encapsulation payload (ESP) and authentication header (AH) services of IPSec, the security delivery element 26 will provide access control, connectionless integrity, data origin
15 authentication, rejection of replayed packets, and confidentiality services. These services will be available for both TCP and UDP streams.

The services delivery element 26 may be configured to communicate in IPSec tunnel mode. In this mode of
20 operation, both the external API 22 and the internal API 18 will authenticate and encrypt the entire IP source packet and wrap a new IP header around them. ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header. AH in tunnel mode
25 authenticates the entire inner IP packet and selected portions of the outer IP header.

Since, as described, the services delivery element 26/
external API 22 IPSec transmissions will be in tunnel mode, all of the hosts inside the core network 10 will
30 communicate with the external API 22 without implementing IPSec. The unprotected packets generated by core network elements are tunneled through the services delivery element

26 by tunnel security associations. The internal APIs 18 may interact with the services delivery element 26 via the embedded security layer on the services delivery element 26. This level of security is implemented to authenticate and validate each particular external API 22.

In accordance with the preferred embodiments of the invention, the services delivery element 26 may be configured to recognize particular external APIs 22. For example, one third party vendor may have more access to the core network 10 than others. Such recognition may be based upon being a known services provider, type of service, or other criteria. Establishing such other criteria will be easily recognized by one having ordinary skill in the art. In this arrangement, the services API 24 will interact with the services delivery element 26 via the embedded Security Layer on the security delivery element 26. This level of security is implemented to authenticate and validate each particular external element, and provide an explicit security layer between the external elements and the core network 10.

External elements (e.g., Feature Server 606 (FIG. 6)) accessing the system via the External APIs 22 may be statically or dynamically associated with the core network 10. For external services that are expected to be delivered to numerous subscribers the operator may configure the core network 10 so that the external API 22 associated with the external service remains statically connected to the core network 10 via this security technique at system initialization. In a dynamic case, when a subscriber requests a particular feature provided by an external element, the core network 10 interrogates the external element.

The associated external API 22 registers with the service delivery element 26, and the services delivery element 26 will authenticate the external element and grant the particular external API 22 access privileges based on this authentication. At this point the external element becomes a trusted element by obtaining the security information. This implies that an additional layer of software must be considered in addition to the external API 22 or that the external API 22 has a local component, which adds the security parameter. A failed security check results in the call to the external API 22 returning an exception.

It will be appreciated that the service delivery element 26 may apply additional or alternate treatments in the event of a failed security check. The treatment applied may depend on the context of the security check failure. For example, a service usage accounting record may be created for the attempted service request. The record could be populated with specific information regarding the attempt and the reason for the security check failure, i.e., the denial of services. In the event the incoming request involves an external caller trying to reach the mobile unit 14 or access data held within the service delivery element 26, additional treatments may be applied. By way of example, an external caller attempting to access the mobile unit 14, but denied access, may be connected to a recorded announcement or progress tone to convey the reason that the access was not granted. The external caller might also be directed to a web page to provide additional information about the failed access attempt.

-10-

The foregoing arrangement is illustrated in FIG. 4. An external feature server 402 and its associated services API 404 are coupled via a message layer 406 to a security layer 408. The security layer 408 interfaces via the
5 external services API 24 to the services delivery element 26.

Once the external element is trusted to the services delivery element 26 a subscriber may attempt to access a given feature provided by the external element. At this
10 point, the core network 10 has access to the external element 402 via its associated API 404 and the security delivery element 26, but the subscriber does not have direct access, i.e., security rights, to the feature offerings of the external element. The subscriber requests
15 the feature and then the services delivery element 26 passes a token on behalf of the subscriber to the external element. The token exchange, shown pictorially in FIG. 5, occurs at the start of the service dialog to enable a particular feature server 502 and its associated services
20 API 504 and the associated service data to support the feature. Service data may be subscriber data such as profile information, location data, etc. An access token 506 is passed between the external API 22 and the services API 504 containing the service request data. It will be
25 appreciated that there may be multiple levels of security checks before this data can be delivered outside the core network 10.

The token exchange and associated authentication lasts for the duration of the dialogue. It should be noted that
30 the dialogue might be a single service request or equivalent to a registration, which may persist over a number of hours. The first external API call establishes

the security relationship between the requestor and the external element. For the lifetime of the relationship, the subsequent external API calls are considered as being sourced by a trusted element. This assumes that the requestor has additional software to support the security check.

Once a security relationship has been established, an external element may need to gain access to additional resources or data within the core network 10. The service API 22 will allow an explicit renegotiation of the security relationship to expand the access granted the external element. This process may also be applied in a reverse fashion to limit the access granted to the external element. For long-lived security relationships, the relationship may be aged to ensure release of the relationship after a predetermined time. This time out period may also be combined with some other criteria, such as inactivity. Once the time out period has expired the external element would be required to re-establish its secure relationship as described herein.

Because services are being provided by external elements, each external element may not use a protocol that is entirely compatible with the internal APIs and/or the core network 10. The services delivery element 26 includes translation functions 304 and API modules 306 (FIG. 3) that translate the service requests from external elements to the known internal API services. This translation function will operate similar to a broker function, a protocol adapter, or a protocol gateway function. The available services will be determined by the authentication services of the security services offered by the services delivery element 26. For example, Java Telephony Application

-12-

Interface (JTAPI) may be supported external to the core network 10 via a translation function 304 within the services delivery element 26. Other translation protocols that may be supported include PARLAY, Telephony Application Interface (TAPI), Java Advanced Intelligent Network (JAIN) and Telecommunication Information Networking Architecture (TINA), which are illustrated in FIG. 3.

The invention may be further illustrated by three use cases, of which two are illustrated in FIG. 6.

1. An external element 602 is hosted in the End User Services Network 604 co-located within the core network 10,
2. An external element 606 is located in or attached to a non-trusted, external network 608 such as the internet, and
3. An external element is located in a trusted or non-trusted external network such as a private service provider network (not shown in FIG. 6).

In the first case, the end-user services network 604 is a trusted entity in a trusted network within the core network 10. In this case the relationship implies a trusted external element accessible over a trusted link. The external element 602 is either imbedded in the trusted network or is represented as a trusted core network 10 entity. This case can be thought of as one where certain classes of services such as three-way voice calling, voice call forwarding, paging, electronic mail, and other "typical" services may be provisioned within the core network 10. As a result, trust is static and requires only service level access security per subscriber.

In the second case, the external element 606 resides in a network 608 attached to the Internet. In this case neither the link to the network 608 where the external element 606 resides

-13-

nor the external element 606 itself is considered trusted. A secure link 610 between the core network 10 and the Internet point of attachment to the packet gateway 612 of the core network 10 must first be established followed by secure access between

5 the mobile unit 14 and the external element 606. As shown in FIG. 6, the mobile unit 14 is provided access to the core network 10 via a trusted element, the services client 614 internal to the core network 10. If there is need for access to resources contained within the core network 10, secure access via security

10 associations 616 is established between the internal APIs 18 and the external element 606, which would automatically invoke the security services in the services delivery element 26. The reverse case, where the external element 606 attempts unsolicited contact with a mobile unit 14, would require the external element

15 establish a secure link with the core network 10 followed by successful security negotiation with the internal API 18 for service discovery. This would be necessary for actions such as subscriber endpoint location and discovery of subscriber device attributes and/or capabilities.

20 In the third case, the external element resides in an external, trusted, private network. This allows statically or dynamically negotiated trust between networks and between an external element and the core network 10 internal APIs 18 to be negotiated jointly or independently using persistent (i.e.,

25 logically or physically) or short-lived link states.

The present invention has been described in terms of several preferred embodiments. It will be appreciated that the invention may be altered or changed without departing from its fair scope. For example, the invention may be applied where an

30 external element, such as an external API, is utilized for remote configuration of elements associated with the core network. Such an implementation would find beneficial use in a system permitting subscriber profile provisioning from a device other than the subscriber device itself. The layered restrictions

possible through application of the services delivery element are advantageously utilized to increase or decrease authorization criteria, which may be leveraged to offer an external element for remote configuration. Thus, an external element may have
5 administrative access to the system from an untrusted source.

The preferred embodiments of the invention are intended to be illustrative and should not be taken as limiting of the broad scope of the invention set forth in the following claims.

100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1089 1090 1091 1092 1093 1094 1095 1096 1097 1098 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1110 1111 1112 1113 1114 1115 1116 1117 1118 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1190 1191 1192 1193 1194 1195 1196 1197 1198 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1290 1291 1292 1293 1294 1295 1296 1297 1298 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1390 1391 1392 1393 1394 1395 1396 1397 1398 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1410 1411 1412 1413 1414 1415 1416 1417 1418 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489 1490 1491 1492 1493 1494 1495 1496 1497 1498 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1510 1511 1512 1513 1514 1515 1516 1517 1518 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1589 1590 1591 1592 1593 1594 1595 1596 1597 1598 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1610 1611 1612 1613 1614 1615 1616 1617 1618 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1689 1690 1691 1692 1693 1694 1695 1696 1697 1698 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1710 1711 1712 1713 1714 1715 1716 1717 1718 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1789 1790 1791 1792 1793 1794 1795 1796 1797 1798 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1810 1811 1812 1813 1814 1815 1816 1817 1818 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1890 1891 1892 1893 1894 1895 1896 1897 1898 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1910 1911 1912 1913 1914 1915 1916 1917 1918 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2189 2190 2191 2192 2193 2194 2195 2196 2197 2198 2199 2200 2201 2202 2203 2204 2205 2206 2207 2208 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219 2220 2221 2222 2223 2224 2225 2226 2227 2228 2229 2230 2231 2232 2233 2234 2235 2236 2237 2238 2239 2240 2241 2242 2243 2244 2245 2246 2247 2248 2249 2250 2251 2252 2253 2254 2255 2256 2257 2258 2259 2260 2261 2262 2263 2264 2265 2266 2267 2268 2269 2270 2271 2272 2273 2274 2275 2276 2277 2278 2279 2280 2281 2282 2283 2284 2285 2286 2287 2288 2289 2290 2291 2292 2293 2294 2295 2296 2297 2298 2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2320 2321 2322 2323 2324 2325 2326 2327 2328 2329 2330 2331 2332 2333 2334 2335 2336 2337 2338 2339 2340 2341 2342 2343 2344 2345 2346 2347 2348 2349 2350 2351 2352 2353 2354 2355 2356 2357 2358 2359 2360 2361 2362 2363 2364 2365 2366 2367 2368 2369 2370 2371 2372 2373 2374 2375 2376 2377 2378 2379 2380 2381 2382 2383 2384 2385 2386 2387 2388 2389 2390 2391 2392 2393 2394 2395 2396 2397 2398 2399 2400 2401 2402 2403 2404 2405 2406 2407 2408 2409 2410 2411 2412 2413 2414 2415 2416 2417 2418 2419 2420 2421 2422 2423 2424 2425 2426 2427 2428 2429 2430 2431 2432 2433 2434 2435 2436 2437 2438 2439 2440 2441 2442 2443 2444 2445 2446 2447 2448 2449 2450 2451 2452 2453 2454 2455 2456 2457 2458 2459 2460 2461 2462 2463 2464 2465 2466 2467 2468 2469 2470 2471 2472 2473 2474 2475 2476 2477 2478 2479 2480 2481 2482 2483 2484 2485 2486 2487 2488 2489 2490 2491 2492 2493 2494 2495 2496 2497 2498 2499 2500 2501 2502 2503 2504 2505 2506 2507 2508 2509 2510 2511 2512 2513 2514 2515 2516 2517 2518 2519 2520 2521 2522 2523 2524 2525 2526 2527 2528 2529 2530 2531 2532 2533 2534 2535 2536 2537 2538 2539 2540 2541 2542 2543 2544 2545 2546 2547 2548 2549 2550 2551 2552 2553 2554 2555 2556 2557 2558 2559 2560 2561 2562 2563 2564 2565 2566 2567 2568 2569 2570 2571 2572 2573 2574 2575 2576 2577 2578 2579 2580 2581 2582 2583 2584 2585 2586 2587 2588 2589 2590 2591 2592 2593 2594 2595 2596 2597 2598 2599 2600 2601 2602 2603 2604 2605 2606 2607 2608 2609 2610 2611 2612 2613 2614 2615 2616 2617 2618 2619 2620 2621 2622 2623 2624 2625 2626 2627 2628 2629 2630 2631 2632 2633 2634 2635 2636 2637 2638 2639 2640 2641 2642 2643 2644 2645 2646 2647 2648 2649 2650 2651 2652 2653 2654 2655 2656 2657 2658 2659 2660 2661 2662 2663 2664 2665 2666 2667 2668 2669 2670 2671 2672 2673 2674 2675 2676 2677 2678 2679 2680 2681 2682 2683 2684 2685 2686 2687 2688 2689 2690 2691 2692 2693 2694 2695 2696 2697 2

CLAIMS

1. An apparatus for interfacing a communication network
5 to an external element comprising:
an interface device coupled to the communication
network and the external element, the interface device
comprising a processor adapted to operate responsive to a
control program stored within a memory associated with the
10 processor; and wherein the interface device is operable to
recognize the external element, to negotiate a security
level between the external element and the communication
network, and to manage access by the external element to
the communication network.
- 15 2. The apparatus of claim 1, wherein the security level
defines a level of access of the external element to the
communication network.
- 20 3. The apparatus of claim 1, wherein, based upon the
security level, the interface device restricts access by
the external element to at least one class of data retained
within the communication network.
- 25 4. The apparatus of claim 1, wherein, based upon the
security level, the interface device restricts access by
the external element to at least one internal function of
the communication network.

-16-

5. The apparatus of claim 1, wherein based upon the security level, the interface device terminates access by the external element.

5 6. The apparatus of claim 1, wherein the interface device provides scalable levels of access to the communication network by the external element.

10 7. The apparatus of claim 1, wherein the interface device includes restriction criteria associated with varying degrees of authorization to the communication network by the external element.

15 8. The apparatus of claim 7, wherein the restriction criteria comprises one of user based privileges and network operation variables.

20 9. The apparatus of claim 1, wherein the interface device is operable to provide one of access control, connectionless integrity, data origin authentication, replay packet rejection and confidentiality services.

25 10. The apparatus of claim 1, wherein the interface device includes a tunnel communication mode.

11. The apparatus of claim 10, wherein the tunnel communication mode comprises of an IP security protocol tunnel mode.

30 12. The apparatus of claim 1, wherein the interface device is configured to recognize a particular external element.

-17-

13. The apparatus of claim 1, wherein the interface device comprises an embedded security layer.

14. The apparatus of claim 1, wherein the interface device
5 establishes a security layer between the communication network and the external element.

15. The apparatus of claim 1, wherein the interface device is operable to establish one of a static association and a
10 dynamic association between the external element and the communication network.

16. The apparatus of claim 1, wherein the interface device is operable to establish both a static association and a
15 dynamic association between the external element and the communication network at the same time.

17. The apparatus of claim 1, wherein the interface device is operable to provide an action responsive to the security
20 level.

18. The apparatus of claim 17, wherein the action comprises one of creating a usage accounting record and providing a message.
25

19. The apparatus of claim 1, wherein the interface device is operable to expand access to the communication network by the external element.

20. The apparatus of claim 19, wherein the interface
30 device expands access to the communication network by the

external element subsequent to a renegotiation of the security level.

21. The apparatus of claim 1, wherein the interface device
5 comprises a translation function.

22. A method of interfacing a communication network to an external element comprising the steps of:

providing an interface coupled between the
10 communication network and the external element,
recognizing the external element via the interface,
negotiating a security level between the external
element and the communication network, and
metering access via the interface by the external
15 element to the communication network in view of the
security level.

23. The method of claim 22, wherein the security level
defines a level of access of the external element to the
20 communication network.

24. The method of claim 22, wherein the method comprises,
based upon the security level, restricting access by the
external element to at least one class of data retained
25 within the communication network.

25. The method of claim 22, wherein the method comprises,
based upon the security level, restricting access by the
external element to at least one internal function of the
30 communication network.

26. The method of claim 22, wherein the method comprises, based upon the security level, terminating access to the communication network by the external element.

5 27. The method of claim 22, further comprising scaling levels of access to the communication network by the external element.

10 28. The method of claim 22, wherein the interface device includes restriction criteria, and wherein the method comprises varying degrees of authorization to the communication network by the external element in view of the restriction criteria.

15 29. The method of claim 28, wherein the restriction criteria comprises one of user based privileges and network operation variables.

20 30. The method of claim 22, the method comprising tunneling data between the external element and the communication network through the interface device.

25 31. The method of claim 22, wherein the step of recognizing an external element comprises recognizing a particular external element.

32. The method of claim 22, comprising establishing a security layer between the communication network and the external element.

33. The method of claim 22, comprising establishing one of a static association and a dynamic association between the external element and the communication network.

5 34. The method of claim 22, comprising, in response to a failure to negotiate a security level, providing an action responsive to the failure to negotiate a security level.

10 35. The method of claim 34, wherein the action comprises one of creating a usage accounting record, providing a recorded message and linking to a source of additional information.

15 36. The method of claim 22, comprising expanding access to the communication network by the external element.

20 37. The method of claim 22, wherein the step of expanding access to the communication network by the external element comprises renegotiating the security level.

25 38. The method of claim of claim 22, further comprising the step of translating data communicated between the external element and the communication network.

Abstract of the Disclosure

[illegible]

┌

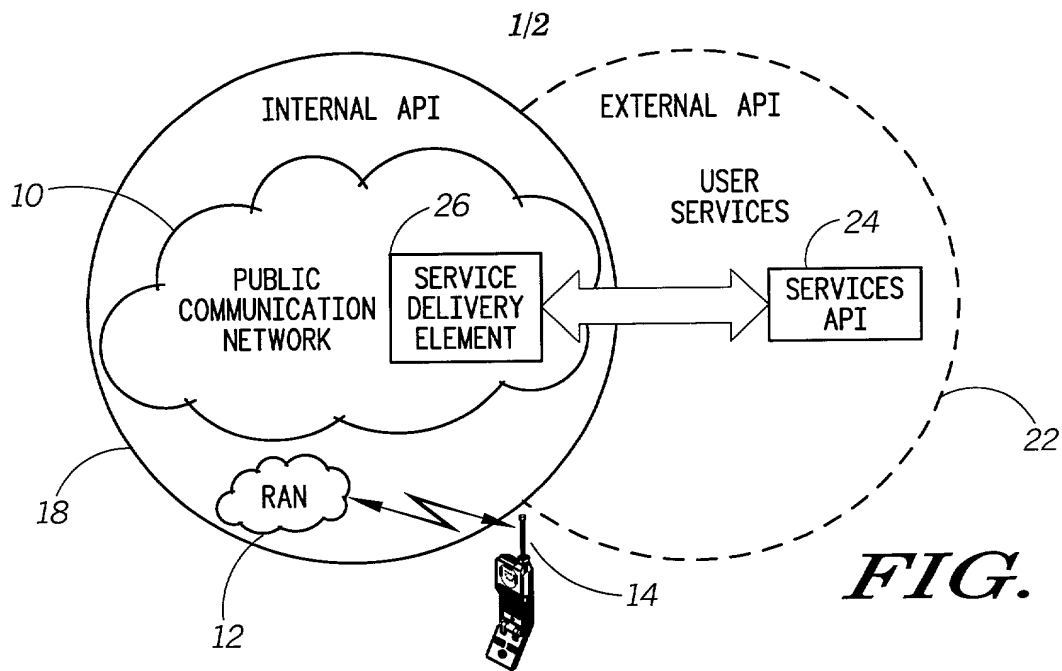


FIG. 1

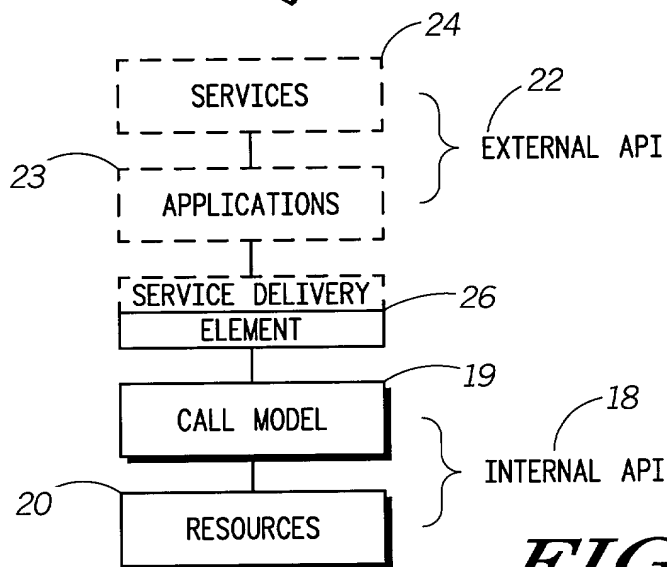


FIG. 2

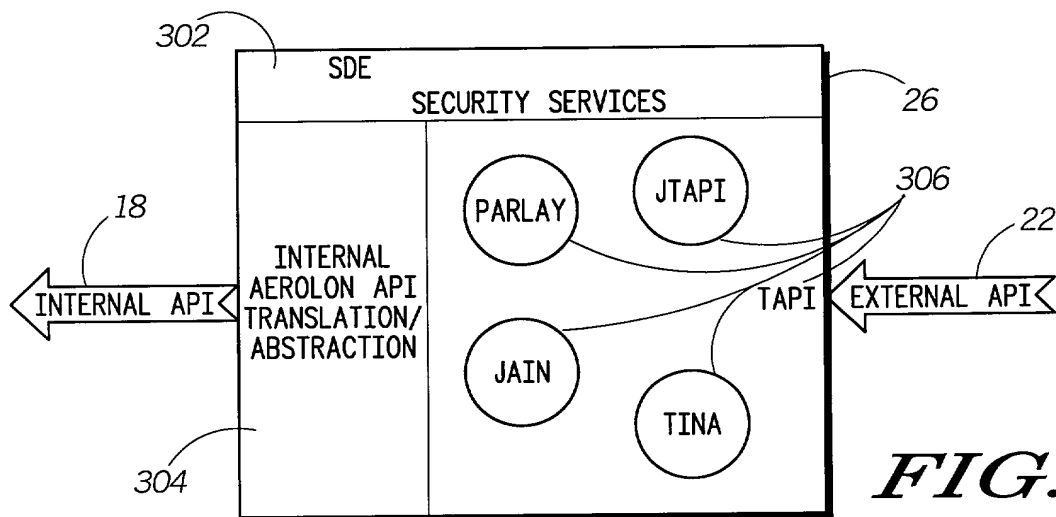
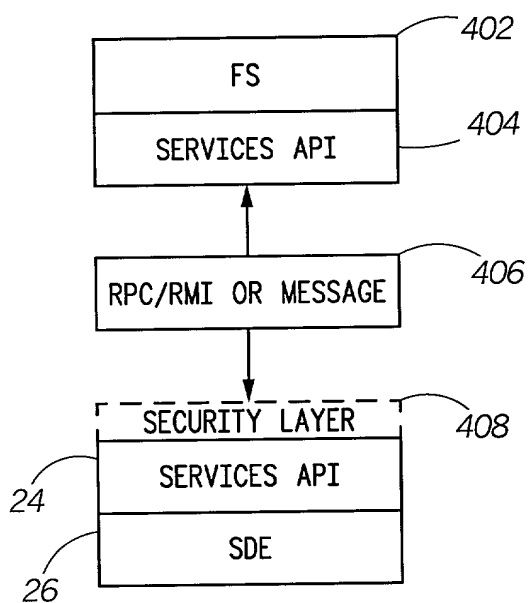
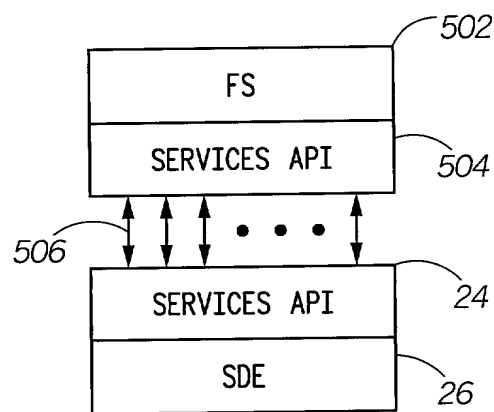
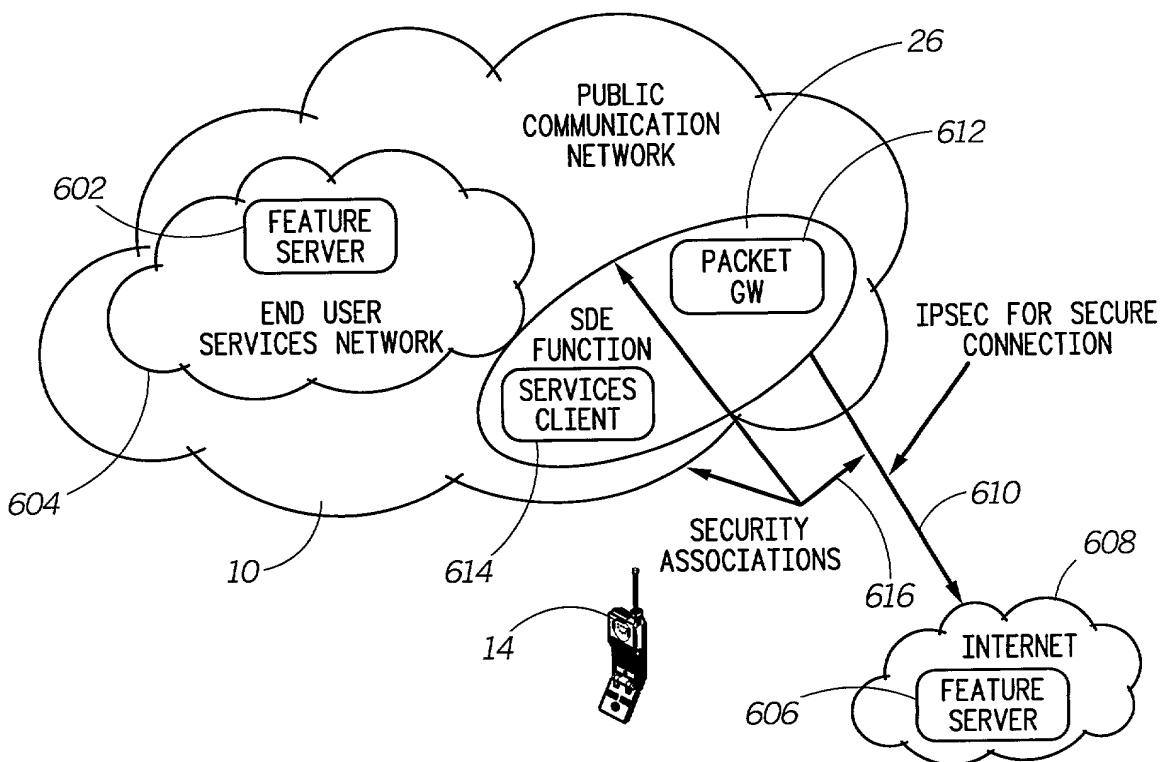


FIG. 3

└

**FIG. 4****FIG. 5****FIG. 6**

PATENT APPLICATION DECLARATION
COMBINED WITH POWER OF ATTORNEY

Attorney's Docket No.: CE08314R



Regular (Utility)



Design Application

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND APPARATUS FOR INTERFACING A NETWORK TO AN EXTERNAL
ELEMENT

the specification of which:



is attached hereto



was filed on: _____

as U.S. Serial No.: _____

and was amended on _____

(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with 37 CFR § 1.56(a).

I hereby claim foreign priority benefits under 35 U.S.C. § 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):



no such application(s) filed



such application(s) identified as
follows:

Application Number	Country	Date of Filing (day, month, year)	Priority Claimed	
			<input type="checkbox"/> Yes	<input type="checkbox"/> No
			<input type="checkbox"/> Yes	<input type="checkbox"/> No

CE08314R

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below:

Provisional Application Serial No.: _____

Provisional Application Filing Date: _____

I hereby claim the priority benefit under 35 USC §120 of any United States application(s), or 365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 USC 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR §1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

Prior U.S. Application(s):



no such application(s) filed



such application(s) identified as follows:

U.S. Parent Application No. or PCT Parent No.	Filing Date (day, month, year)	Status (Patented, Pending, Abandoned)

AS A NAMED INVENTOR, I HEREBY APPOINT THE FOLLOWING REGISTERED ATTORNEY(S) OR AGENT(S) TO PROSECUTE THIS APPLICATION AND TO TRANSACT ALL BUSINESS IN THE PATENT AND TRADEMARK OFFICE CONNECTED THEREWITH:

CUSTOMER NUMBER 22917

Send correspondence to Customer Number **22917**

Address all telephone calls to:

Kenneth A. Haas at (847) 576-0379

Fax (847) 576-3750

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 USC and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first-named or sole inventor <u>ROBERT BANKS</u>		
Inventor's signature	<u><i>Robert Banks</i></u>	Date <u>June 2, 2000</u>
Residence	<u>Barrington</u>	<u>IL</u>
	City	State or Foreign Country
Citizenship	<u>USA</u>	
	Country	
Post Office Address	<u>4921 Lichfield Drive</u>	
	Street Address	
<u>Barrington</u>	<u>IL</u>	<u>60010-5615</u>
City	State or Country	Zip Code

Full name of second-named joint inventor <u>WESLEY STUART JONES</u>		
Inventor's signature	<u><i>Wesley Stuart Jones</i></u>	Date <u>5 JUNE 2000</u>
Residence	<u>Palatine</u>	<u>IL</u>
	City	State or Foreign Country
Citizenship	<u>USA</u>	
	Country	
Post Office Address	<u>643 East Monterey Road</u>	
	Street Address	
<u>Palatine</u>	<u>IL</u>	<u>60067-3725</u>
City	State or Country	Zip Code

Full name of third-named joint inventor RICHARD MALCOLM

Inventor's signature *Richard Malcolm* Date 6/5/00

Residence Carol Stream IL
City State or Foreign Country

Citizenship USA
Country

Post Office Address 625 Paxton Place
Street Address

Carol Stream IL 60188
City State or Country Zip Code